REMARKS/ARGUMENTS

The comments in the Advisory Action has been carefully considered. The issues raised are respectfully submitted to be traversed and addressed below.

""Claim Rejections – 35 USC § 103"

In the continuation sheet of the Advisory Action, the Examiner has maintained his rejections under 35 U.S.C. §103(a), as the Examiner believes that claims 1 to 4, 6 to 15, and 17 to 20 are unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann *et al*, US Patent Number 5,608,800.

The Applicant respectfully submits that the present claim 1 is patentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann *et al*, US Patent Number 5,608,800.

The Applicant respectfully maintains that Sony and Hoffmann are concerned with different security systems, that is, Sony is concerned with authenticating IC cards, and a R/W, and Hoffmann is concerned with validating data, thus, there would be no motivation for a person skilled in the art to combine the two references.

However as the Examiner believes that the references can be combined, the applicant now addresses the combination.

Present claim 1 requires:

1. generating a secret random number;
2. calculating a signature for the random number using a signature function, in a trusted authentication chip;
3. encrypting the random number <u>and</u> the signature by a symmetric encryption function using a first key, in the trusted authentication chip;
4. passing the encrypted random number and the signature from the trusted authentication chip to an untrusted authentication chip;

Sony describes a reader/writer transmitting C1 (code) to an IC card such that a random number RA is encrypted using a key KB (see abstract). With respect to Hoffmann,

Hoffmann describes the transmission of a message from a transmitter SE to a receiver EM, where the message is transmitted by (see column 2 lines 37 to 52):

1. generating random data Z at the transmitter;
2. establishing coupling data K
3. generating a symmetric key E from the combination of the random data Z and the coupling data K by one-way enciphering;
4. generating an enciphered signature S/E by symmetrically enciphering a signature S with the key E;
5. forming an enciphered random data Z/T by using a transfer key T and the random number Z; and,
6. formulating the message to be transmitted, the message including useful data D, enciphered signature S/E, coupling data K, and enciphered random data Z/T.

Thus, a combination of Sony and Hoffmann would describe generating a random number and encrypting the random number with a key, establishing coupling data K, and generating a symmetric key from the combination of the random number and the coupling data K by one way enciphering. The random number is then combined with the coupling data in order to form a symmetric key, which in turn enciphers the signature.

Therefore, a combination of Sony and Hoffmann teaches the signature being enciphered by a key formed from the random number. In contrast, present claim 1 teaches the random number and the signature being enciphered by the same key. This is in no way taught or described by either Sony, or Hoffmann, or a combination thereof.

Secondly, claim 1 further describes once the encrypted random number and signature have been transmitted:

1. decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted authentication chip;
2. comparing the signature calculated in the untrusted authentication chip with the signature decrypted;

Sony further describes that once the reader/writer transmits the code to the IC card:

1. the IC card decrypts code C1 into plain text M1 using key KB.

2. the IC card transmits R/W code C2 such that plain text M1 is encrypted using key KA and code C3 such that a random number RB is encrypted using key KA.
3. R/W decrypts codes C2 and C3 into plain text M2 and plain text M3 using KA.
4. R/W determines plain text M2 and random number RA are the same, therefore authenticates the IC card.
5. R/W transmits to IC card a code C4 such that plain text M3 is encrypted using key KB.

In Hoffmann, once the formed message is transmitted, it is checked at the receiver end by the following steps (see column 3 line 60 to column 4 line 7):

1. checking the coupling data for plausibility, the message is rejected if check;
2. recovering the random data Z by deciphering the enciphered random data Z/T by the use of the transfer key T;
3. determining the symmetric key E from the calculated random data Z and the coupling data K;
4. recovering the signature S by deciphering the enciphering signature S/E by using E; and,
5. checking the signature S for errors, if errors exist then the message is rejected.

Neither Sony, Hoffmann or a combination thereof describe comparing the signature calculated in the untrusted authentication chip with the signature decrypted. Sony describes two untrusted chips, but does not describe comparing the signatures, and Hoffman does not describe the comparing of the signatures in a chip (as Hoffmann is concerned with authenticating messages), Hoffmann only describes checking the signautre for errors. Thus, there is no comparison step in the combination of Sony and Hoffman of comparing signatures, in an untrusted chip.

Thirdly, claim 1 continues to describe that in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

Sony continues to describe that once the reader/writer transmits to the IC card a code C4 (including plain text M3 encrypted using key KB):

1. IC card decrypts code C4 into plain text M4 using key KB.

2. When IC card determines plain text M4 and random number RB are the same, the R/W is authenticated.

Hoffman describes only one way authentication, and does not return any data. Thus, the combination of Sony and Hoffman would only include the steps described by Sony above, and hence would not describe that in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

Fourthly, claim 1 further describes, that once the encrypted random number is returned to the trusted authentication chip:

1. encrypting the random number by the symmetric encryption function using the second key, in the trusted authentication chip;
2. comparing the two random numbers encrypted using the second key, in the trusted authentication chip;
3. in the event that the two random numbers encrypted using the second key match, considering the untrusted chip to be valid, and otherwise, the chip is invalid;

which, neither Sony, Hoffmann, or a combination thereof describe.

Therefore, the combination of Sony and Hoffmann does not describe the use of a first key to encrypt a random number and a signature by a symmetric encryption function, comparing two signatures in an untrusted chip, and in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using the second key an returning it to the trusted authentication chip, and further still, once the data is returned to the trusted authentication chip, encrypting the random number by the symmetric function using the second key, and then comparing the two random numbers.

Hence, the Applicant respectfully submits, that claim 1 recites a different security system to the combination of Sony and Hoffmann. It will be appreciated by the Examiner, that these differences in security systems are not trivial. Thus, claim 1 is patentable over Sony in view of Hoffmann.

CONCLUSION

In light of the above, it is respectfully submitted that the claim rejections have been successfully traversed and addressed. Accordingly, it is respectfully submitted that the claims, and the application as a whole with these claims, are allowable, and a favourable reconsideration is therefore earnestly solicited.

Very respectfully,

Applicant:

Simon Walmsley
SIMON ROBERT WALMSLEY

Applicant:

PAUL LAPSTUN

C/o:
Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762